

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-088322

(43)Date of publication of application : 30.03.1999

(51)Int.Cl. H04L 9/32  
G06T 7/00  
G09C 1/00  
// A61B 5/117

(21)Application number : 09-236927

(71)Applicant : KIYADEITSUKUSU:KK

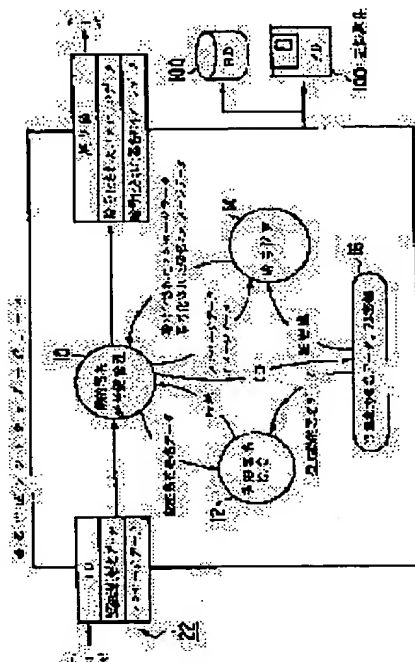
(22)Date of filing : 02.09.1997

(72)Inventor : TABUKI TAKAAKI

**(54) DIGITAL SIGNATURE GENERATION METHOD****(57)Abstract:**

**PROBLEM TO BE SOLVED:** To provide a digital signature system full of convenience for easily managing a secret key in a digital signature utilizing a public key cipher system.

**SOLUTION:** Based on an 'ID' transmitted from a user, a dynamic signature cipher key management module 10 obtains registered dynamic signature data and the secret key from an array management module 16. The registered dynamic signature data and authentication dynamic signature data transmitted from the user are collated in a dynamic signature collation module 12. In the case of judging that both are the same signature data, the dynamic signature cipher key management module 10 supplies message data transmitted from the user and the secret key to a cipher computing module 14 and the cipher computing module 14 transmits the message data or the like ciphered by the secret key to the dynamic signature cipher key management module 10. The dynamic signature cipher key management module 10 sends back the ciphered, that is signed, message data or the like to the user. Since the secret key is buried in a program, even when the program is copied, a misuse by a third person is not invited.

**LEGAL STATUS**

[Date of request for examination] 09.08.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office



## 【特許請求の範囲】

【請求項1】デジタル署名の対象であるメッセージデータと、前記デジタル署名を要求するユーザの識別子と、前記ユーザの生体署名データと、を入力する入力ステップと、

前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得ステップと、

前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査ステップと、

前記検査ステップにおいて、前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でデジタル署名を施すデジタル署名ステップと、

を含むことを特徴とするデジタル署名生成方法。

【請求項2】請求項1記載のデジタル署名生成方法において、

前記登録生体署名データ取得ステップは、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることの特徴とするデジタル署名生成方法。

【請求項3】請求項1記載のデジタル署名生成方法において、

前記登録生体署名データ取得ステップは、同一ユーザが複数の識別子を所有することを許容することの特徴とするデジタル署名生成方法。

【請求項4】請求項1、2又は3記載のデジタル署名生成方法において、

前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするデジタル署名生成方法。

【請求項5】請求項1、2又は3記載のデジタル署名生成方法において、

前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするデジタル署名生成方法。

【請求項6】請求項1、2又は3記載のデジタル署名生成方法において、

前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするデジタル署名生成方法。

【請求項7】請求項5記載のデジタル署名生成方法において、

前記入力された生体署名データである前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換ステップと、

前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名ステップと、

を含むことを特徴とするデジタル署名生成方法。

【請求項8】デジタル署名の対象であるメッセージデータと、前記デジタル署名を要求するユーザの識別子

と、前記ユーザの生体署名データと、を入力する入力手順と、

前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得手順と、

前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否か検査する検査手順と、

前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でデジタル署名を施すデジタル署名手順と、

を含むプログラムを格納したコンピュータ読みとり可能な記憶媒体。

【請求項9】請求項8記載のコンピュータ読みとり可能な記憶媒体において、

前記登録生体署名データ取得手順は、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることの特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。

【請求項10】請求項8記載のコンピュータ読みとり可能な記憶媒体において、

前記登録生体署名データ取得手順は、同一ユーザが複数の識別子を所有することを許容することの特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。

【請求項11】請求項8、9又は10記載のコンピュータ読みとり可能な記憶媒体において、

前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。

【請求項12】請求項8、9又は10記載のコンピュータ読みとり可能な記憶媒体において、

前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。

【請求項13】請求項8、9又は10記載のコンピュータ読みとり可能な記憶媒体において、

前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。

【請求項14】請求項11記載のコンピュータ読みとり可能な記憶媒体において、

前記プログラムは、

前記入力された生体署名データであるデータであって、前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換手順と、

前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名手順と、

を含むことを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、公開鍵暗号方式に関する。特に、公開鍵暗号方式を用いてデジタル署名を行う方法に関する。

## 【0002】

【従来の技術】近年、ネットワークによる通信が発展し、ネットワーク上におけるメッセージの送受信等に暗号化方式が利用される場合も多い。暗号化方式には、古典的な共通鍵方式も用いられているが、鍵の管理が煩雑になる等の理由から、公開鍵暗号方式が用いられてつづける。

【0003】公開鍵暗号方式においては、各人は自己の秘密鍵を秘密に管理し、自己の公開鍵を他人に公開する。そして、他人は、ある個人の公開鍵を用いてメッセージを暗号化してその個人に送る。公開鍵により暗号化されたメッセージは、秘密鍵を知っているその個人のみが復号化できるため、第三者に対してメッセージの内容は秘密に保たれる。

【0004】さらに、この公開鍵暗号方式は、いわゆるデジタル署名を容易に行うことができるという特徴を有している。

【0005】すなわち、ある甲が所定のメッセージについて自己の署名を行う場合には、そのメッセージに対して甲の秘密鍵で暗号化を行う。この秘密鍵で暗号化したメッセージは甲の公開鍵でのみ復号化できる。そのため、だれでも、甲の公開鍵でそのメッセージを復号化し、もとのメッセージの内容を確認することができる。甲の公開鍵で復号化できるのは、甲の秘密鍵で暗号化した文章だけである。従って、甲の公開鍵で復号化できたことは、甲が確かにそのメッセージに対して甲の秘密鍵を用いて暗号化したことを意味する。そして、甲の秘密鍵を知っているのは甲のみであるため、このような暗号化ができるのは甲のみである。

【0006】このように、甲のみが行える処理を他人が確認できるため、この処理をもって甲の「署名」と見なすことができる。

【0007】さて、このようなデジタル署名をはじめとして、公開鍵暗号方式においては、秘密鍵はその所有者のみが知っている必要がある。すなわち、秘密鍵は各個人が個人の責任において厳重に管理しなければならない。

【0008】ところが、近年用いられている公開鍵暗号方式に用いられる鍵の長さは、暗号強度を保つために500ビットから1000ビット程度のものが用いられ又は提案されている。

【0009】数桁程度のパスワードのようなものならばともかく、このような500ビットや1000ビット程度のデータは、人間が容易に覚えられないものではない。そこで、一般には公開鍵暗号方式の秘密鍵はコンピュー

タ内のハードディスクに保存したり、ICカード内に記憶させておくことがなされている。

【0010】しかし、秘密鍵をコンピュータ内のハードディスク等に格納した場合には、誰でもその秘密鍵を利用することができる可能性がある。そのため、一般にはそのハードディスク内に格納した秘密鍵は、パスワードによるプロテクトが施されている場合が多い。すなわち、その秘密鍵をデジタル署名等に使用する場合にはその利用者はパスワードを入力することにより初めてその秘密鍵を使用できるのである。

## 【0011】

【発明が解決しようとする課題】従来の公開鍵暗号方式の秘密鍵を利用したデジタル署名においては、このように秘密鍵の管理は各個人が行わなければならない、また、具体的にはパスワード等による秘密鍵のプロテクトが行われていた。

【0012】しかし、パスワードは、人間が覚えやすいものである必要があるため、一般には短いものが多く、不注意により他人の目に触れやすい。かつ、一旦目に触れてしまった場合（短いため）覚えられやすいという性質がある。

【0013】このように、従来の秘密鍵の保管は結局の所パスワードの強度に依存していたため、秘密鍵のプロテクトにも自ずと限界があった。その結果、第三者によるいわゆる「なりすまし」を招きやすく、第三者がその正当な権利を有する者になりすまして、デジタル署名を行ってしまう恐れも小さくはなかった。

【0014】さらに、基本的に秘密鍵の管理は、その正当使用者個人の管理に任されている。そのため、例えば法人が使用者であるような「法人鍵」を使用する場合においても結局は個人が秘密鍵の管理を行っている。そのため、秘密鍵の重要度に関係なく、その鍵が個人の鍵であっても法人の鍵であっても、同じような安全度でしか管理されていない。

【0015】その結果、ある企業内部で、個人が重要な法人鍵を不正に使用してしまう可能性は、個人の鍵が不正に使用されてしまう可能性とほとんど変わらないのが現状である。

【0016】また、近年、企業においては法人が秘密鍵の所有者になること、すなわちその企業を表す鍵が望まれている。このような法人鍵は、いわば従来の法人の印章に相当するものである。このような法人鍵は、その法人である企業の各社員が使用する性質のものである。しかし、1つの秘密鍵を特定の個人だけが使用することを前提としている現在の公開鍵暗号方式の実現手法では、1個の法人鍵を複数人で使用する形態については何ら考慮されてはいない。このことは換言すれば1個の秘密鍵をその本人（法人）の代理人が使用する仕組みが、未だ構築されていないことを意味している。

【0017】本発明は、以上のような課題を解決するた

めになされたものであり、その目的は、企業等において、各個人がデジタル署名を行う場合に、不正な使用を確実に防止するためのデジタル署名のための方法を構築することである。

【0018】

【課題を解決するための手段】本発明はデジタル署名のための方法に関するものであり、本発明において特徴的なことは、IDやパスワードなどの他に、生体署名データを用いて各人の識別を行っているため、より正確に各個人の識別を可能としていることである。

【0019】また、本発明において特徴的なことは、複数の秘密鍵が、複数の人によって使用され得る点にある。このようなデジタル署名の手法を実現するために、記憶手段内には、複数のユーザ対複数の秘密鍵、のデータ構造が構築されている。

【0020】従来の技術においては、秘密鍵はあくまでも1人の人間によって所有・管理されていた。しかし、そのため、その1人のみが使用できる仕組みを構築していたので、上述したようにパスワードを盗まれることによる不正使用（なりすまし等）を招くおそれがあったのである。

【0021】本発明は、複数の秘密鍵が複数人によって使用される方式を実現するデジタル署名生成方法を提供している。具体的には、以下のような手段を採用している。

【0022】本発明は、上記課題を解決するために、デジタル署名の対象であるメッセージデータと、前記デジタル署名を要求するユーザの識別子と、前記ユーザの生体署名データと、を入力する入力ステップと、前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得ステップと、前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否かを検査する検査ステップと、前記検査ステップにおいて、前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でデジタル署名を施すデジタル署名ステップと、を含むことを特徴とするデジタル署名生成方法である。

【0023】生体署名データとは、個人を特定するためのいわゆるBiometricsなデータであり、指紋や網膜パターンなどが使用される。特に、以下に述べる実施形態では種々のメリットがあることから署名データが使用されている。

【0024】また、本発明は、前記登録生体署名データ取得ステップは、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることを特徴とするデジタル署名生成方法である。

【0025】異なるユーザに対して同一の秘密鍵を提供することができ、例えば法人鍵などの管理を容易に行えるものである。

【0026】また、本発明は、前記登録生体署名データ取得ステップは、同一ユーザが複数の識別子を所有することを許容することを特徴とするデジタル署名生成方法である。

【0027】1人のユーザでも役職を複数有する場合も多い。このような場合に、役職毎にデジタル署名を変える必要がある。したがって、本発明においては同一ユーザでも複数の識別子（IDとも呼ぶ）を有することを認め、1人のユーザが複数の秘密鍵を使用できるようにしている。

【0028】また、本発明は、前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするデジタル署名生成方法である。

【0029】また、本発明は、前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするデジタル署名生成方法である。

【0030】また、本発明は、前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするデジタル署名生成方法である。

【0031】また、本発明は、前記入力された生体署名データである前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換ステップと、前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名ステップと、を含むことを特徴とするデジタル署名生成方法である。

【0032】イメージデータをも秘密鍵を用いて署名したので、従来の手で行う署名のイメージを利用することができ、従来のシステムとの類似性を維持することができる。

【0033】また、本発明は、これまで述べた方法に関する発明を実現するプログラムを格納したコンピュータ読みとり可能な記憶媒体に関する。

【0034】具体的には、以下のような手順を実行するプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【0035】本発明は、デジタル署名の対象であるメッセージデータと、前記デジタル署名を要求するユーザの識別子と、前記ユーザの生体署名データと、を入力する入力手順と、前記ユーザの識別子に基づき、前記ユーザの予め登録された登録生体署名データを取得する登録生体署名データ取得手順と、前記生体署名データと、前記ユーザの登録された登録生体署名データとを比較し、両者の特徴量が一致するか否かを検査する検査手順と、前記両者の特徴量が一致した場合にのみ、前記メッセージデータに対し、前記ユーザの秘密鍵でデジタル署名を施すデジタル署名手順と、を含むプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【0036】また、本発明は、前記登録生体署名データ取得手順は、異なるユーザの識別子に対して、同一の秘密鍵を取得しうることを特徴とするプログラムを格納し

たコンピュータ読みとり可能な記憶媒体である。

【0037】また、本発明は、前記登録生体署名データ取得手順は、同一ユーザが複数の識別子を所有することを許容することを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【0038】また、本発明は、前記生体署名データは、ユーザが手で書いた署名に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【0039】また、本発明は、前記生体署名データは、前記ユーザの網膜パターンに関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【0040】また、本発明は、前記生体署名データは、前記ユーザの指紋に関するデータであることを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【0041】また、本発明は、前記プログラムは、前記入力された生体署名データであるデータであって、前記ユーザが手で書いた署名に関するデータを、イメージデータに変換する変換手順と、前記イメージデータに対し、前記秘密鍵を用いて署名を施すイメージデータ署名手順と、を含むことを特徴とするプログラムを格納したコンピュータ読みとり可能な記憶媒体である。

【0042】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基いて説明する。

【0043】本実施の形態においては、ユーザが利用するコンピュータ上において、ユーザのID等だけでなく、ユーザの認証動的署名データに基づいて、ユーザの識別を行い、識別したユーザの秘密鍵を用いてデジタル署名を行ったものである。

【0044】具体的には、本実施の形態は、コンピュータ上で動作するプログラムで実現されている。

【0045】本実施の形態に係るプログラムの各モジュールの構成図が図1に示されている。この図に示されているように、動的署名暗号鍵管理モジュール10と、動的署名照合モジュール12と、暗号演算モジュール14と、配列管理モジュール16と、が本プログラムに含まれている。

【0046】本実施の形態においては、これらのモジュールを含むプログラムを用いて、そのコンピュータのユーザの要求に応じて、所定のメッセージデータに対し署名を行っている。

【0047】入力信号

本プログラムの具体的な動作を説明する前に、プログラムに入力する信号に関する説明を中心に本実施形態の特徴を述べる。

【0048】このプログラムに対する入力22は、図1に示すように、ユーザの「ID」と、ユーザの「認証動

動的署名データ」と、そのユーザが署名を受けたい「メッセージデータ」と、を含んでいる。本プログラムは、そのユーザの秘密鍵を用いて、「メッセージデータ」を暗号化することによって「メッセージデータ」に署名をする。そして、「暗号化された（署名された）メッセージデータ」が出力されるのである。

【0049】ここで、認証動的署名データとは、そのユーザの「手で書いた署名」のデータや、指紋、網膜パターンなどのいわゆるBiometricsな個人特定データである。本実施の形態においては、例えば、認証を利用したい者がそのコンピュータに周辺機器等として備えられているタブレット上でスタイラスペンなどを用いて「手で書いた署名」をする事により、認証動的署名データが入力される。

【0050】さて、本プログラムの入力22の「認証動的署名データ」とは、ユーザがデジタル署名を行いたい場合に入力した動的署名データである。上述したように、例えば端末のタブレットなどから、そのユーザの「手で書いた署名」のデータなどが、この「認証動的署名データ」として利用される。

【0051】この「認証動的署名データ」は、配列管理モジュール16において配列中に予め格納されている「登録動的署名データ」と、比較照合される。実際の比較照合処理は、動的署名照合モジュール12で行われる。このように、本実施の形態においては、生体データを用いて本人であるか否かの検査を行っているので、本人以外の人間による不正なデジタル署名を効果的に防止することができる。この検査処理の流れに関しては、後において詳述する。

【0052】また、図1に示されているように、本プログラムは、配列管理モジュール16を有している。この配列管理モジュール16においては、各個人（の「ID」）とその個人が使用する「秘密鍵」の管理が行われている。具体的には「ID」と、「秘密鍵」が配列中に記憶されているのである。さらに、上述した「登録動的署名データ」も、この配列管理モジュール16において、配列中に格納されて管理されている。

【0053】本実施の形態において特徴的なことは、秘密鍵等が、ICカードなどの特定のハードウェア中に記憶されているのではなく、ソフトウェア中に組み込まれていることである。ソフトウェア中に組み込む手法は従来の種々の方法が利用可能であるが、例えば本実施の形態においては、データ配列中にユーザの「ID」や「秘密鍵」等を格納している。

【0054】このように、ソフトウェア中に組み込まれているため、たとえ悪意の第三者に本実施の形態におけるプログラムが盗まれてコピーされても、そのプログラムを悪用すること、例えば間違ったIDを利用して正規の秘密鍵を利用すること等は行えない。その理由は、プログラム中に組み込まれた「ID」や「秘密鍵」の内容

を書き換えることは、そのプログラムの作成者ならば容易であるが、第三者にとっては一般に非常に困難なことだからである。

【0055】本実施の形態において特徴的なことは、秘密鍵の管理がその所有者である個人ではなく、本実施の形態におけるプログラムが集中的に行っていることである。このような手段を講じることによって、そのコンピュータを使用する各人の秘密鍵の管理を集中して行うことができ、煩雑な秘密鍵の管理を個人が行う必要がなくなる。

【0056】尚、本実施の形態においては、「手で書いた署名」データを利用したが、上述したようにこの動的署名データは、指紋や網膜パターンなど、Biometricsに本人を特定しうるデータであればどのようなものでもかまわない。

#### 【0057】動作

次に、本発明のデジタル署名生成方法の動作について、プログラムの処理の流れを中心に説明する。

【0058】本実施の形態におけるプログラムは、これまで述べた、ユーザの「ID」、「認証動的署名データ」、及び「メッセージデータ」から成る入力22が供給されると、まず、動的署名暗号鍵管理モジュール10が、そのIDが表すユーザに対し登録されている「登録動的署名データ」を、配列管理モジュール16から読み出す。図1に示すように、動的署名暗号鍵管理モジュール10は、「ID」を配列管理モジュール16に与える。そして、配列管理モジュール16は、この「ID」をキーとして、配列に格納されているデータの検索を行い、「登録動的署名データ」と「秘密鍵」を出力する。

【0059】さて、配列管理モジュール16が出力した「登録動的署名データ」は、図1に示されているように、動的署名照合モジュール12に供給される。一方、動的署名暗号鍵管理モジュール10も、ユーザが入力した「認証動的署名データ」を動的署名照合モジュール12に供給する。

【0060】動的署名照合モジュール12は、供給された上記「認証動的署名データ」と「登録動的署名データ」との比較・照合を行う。そして、その比較の結果を動的署名暗号鍵管理モジュール10に送信する。

【0061】さて、配列データに格納されている「登録動的署名データ」と、ユーザによって入力された「認証動的署名データ」とがその特徴事項について一致し、共に同一人に対するBiometricsな署名データであると判断される場合には、デジタル署名の要求が正しく行われている（正規のユーザによりデジタル署名が要求されている）と判断される。したがって、この場合は上記比較結果として例えば「正常」を動的署名暗号鍵管理モジュール10に対し送信するのである。この「正常」である旨の比較結果が動的署名暗号鍵管理モジュール10に送信された後は、後に述べるデジタル署名

名の処理が、暗号演算モジュール14において実行される。

【0062】一方、予め配列管理モジュール16に登録されている「登録動的署名データ」と入力された「認証動的署名データ」とがその特徴事項について一致せず、同一人に対するBiometricsな署名データではないと、動的署名照合モジュール12（図1参照）において判断された場合には、この認証の要求は不正行為によって行われた要求であると判断し、本プログラムは、ユーザの要求を拒絶する。具体的には、動的署名暗号鍵管理モジュール10が拒絶のメッセージをユーザに送信するのである。

【0063】さて、動的署名照合モジュール12が、「正常」である旨の結果を動的署名暗号鍵管理モジュール10に送信してきた場合には、動的署名暗号鍵管理モジュール10は、暗号演算モジュール14に対してデジタル署名処理を行わせる。すなわち、暗号演算モジュール14は、秘密鍵による暗号化をメッセージデータに対して施すのである。

【0064】ここで、秘密鍵は、図1に示すように配列管理モジュール16が予め出力している。暗号演算モジュール14は、予め出力されているこの秘密鍵を用いて暗号演算、すなわちデジタル署名を行うことができる。

【0065】図1に示すように、暗号演算モジュール14は、暗号化の対象である「メッセージデータ」を動的署名暗号鍵管理モジュール10から受信する。さらに、本実施の形態においては、暗号化の対象として「メッセージデータ」だけでなく、「イメージデータ」をも暗号演算モジュール14は受信する。そして、これら「メッセージデータ」及び「イメージデータ」の暗号化（署名）が暗号演算モジュール14において行われる。

【0066】この「イメージデータ」とは、ユーザにより入力された「認証動的署名データ」をイメージとして表現したイメージデータである。「認証動的署名データ」は、例えば「手で書いた署名」がユーザにより書かれる際のペンの動きをペンの速度・方向やペンの押圧力等で表した数値データである。そして、この「手で書いた署名」をイメージとして表したデータとは、その署名データ（押圧力等で表した数値データ）を人間に見える形で表すため、上記ペンの動きを2次元の紙の上に再現し、人間の視覚で把握できるようにした画像データである。

【0067】この「認証動的署名データ」をイメージとして表現したイメージデータに変換する処理は、動的署名暗号鍵管理モジュール10において行われる。変換後のイメージデータが図1に示すように暗号演算モジュール14に供給されるのである。

【0068】本実施の形態において、このような署名データのイメージデータをも暗号化している理由は、実際

に肉眼で把握できる形で文章中に署名を表示したいという要求も現実にあるからである。本実施の形態においては、このようにイメージデータをも暗号化したが、このイメージデータの暗号化は、本発明にとっては必ずしも必須の事項ではない。

【0069】暗号演算モジュール14は「メッセージデータ」及び「イメージデータ」を暗号化すると、得られた「暗号化されたメッセージデータ」及び「暗号化された署名のイメージデータ」を出力する。

【0070】動的署名暗号鍵管理モジュール10は、「暗号化されたメッセージデータ」及び「暗号化された署名のイメージデータ」をユーザに返す。これによって、ユーザは、自ら秘密鍵を管理しなくとも、容易に署名を行うことが可能である。特に、本実施の形態においてはIDだけでなく、Biometricsな動的署名データを用いて、本人であることを確認したので、不正に秘密鍵を使用した署名が行われてしまうことを効果的に防止することができる。

【0071】さらに、動的署名暗号鍵管理モジュール10は、図1に示すようにユーザに「戻り値」をも返す。この「戻り値」は、暗号演算の結果を表すいわば「リターンコード」と呼ばれるコードの一種である。

【0072】ユーザは、この「戻り値」の値を検査することにより、暗号演算が正常に終了したのか否か、それとも、IDが表す人物について登録されている登録認証データと認証動的署名データとの特徴事項が一致しなかったのか否か、等について詳細な情報を得ることができる。

【0073】尚、本実施の形態において、本発明のデジタル署名生成方法の各要素は、プログラムで実現されている。

【0074】具体的には、動的署名暗号鍵管理モジュール10は、入力ステップ等に相当する。また、動的署名暗号鍵管理モジュール10は、動的署名照合モジュール12との共同作用で、本発明の検査ステップを実現する。また、動的署名暗号鍵管理モジュール10は、配列管理モジュール16との共同作用で、本発明の登録動的署名データ取得ステップを実現する。また、動的署名暗号鍵管理モジュール10は、暗号演算モジュール14との共同作用で、本発明のデジタル署名ステップを実現する。

【0075】また、動的署名暗号鍵管理モジュール10は、イメージデータへの変換を行う本発明の変換ステップを実現する。

【0076】さらに、本実施の形態における、上記モジュールから成るプログラムは、コンピュータが稼働していないときはコンピュータ読みとり可能な記憶媒体100に格納されている。この記憶媒体100は、ハードディスクを用いるのが一般的であると考えられるが、フロッピーディスクや光ディスクなど、コンピュータ読みと

り可能な記憶媒体であればどのようなものでも使用可能である。

#### 【0077】配列の内容

次に、上記配列管理モジュール16で用いている配列の内容について説明する。

【0078】図2には上記配列管理モジュール16で用いている2種類の配列の内容を表す説明図が示されている。図2(1)には、個人情報管理配列20aが示されており、図2(2)には、暗号鍵管理配列20bが示されている。

【0079】図2(1)に示すように、個人情報管理配列20aは、ユーザの「ID」と、「登録動的署名データ」と、「鍵ハッシュ値」とを格納している配列である。この「鍵ハッシュ値」とは秘密鍵を、所定のハッシュ関数でハッシュ値に変換したものであり、このハッシュ値は、後述する暗号鍵管理配列20bにおいて利用される。ハッシュ値を使用しているのは、上述したように秘密鍵の長さが500ビット〜1000ビット程度であるため、秘密鍵の値そのもので配列の検索を行うと検索時間が長くなってしまうからである。

【0080】さて、本実施の形態においては、ユーザを認識するためにそのユーザの「ID」を用いている(図2(1)参照)。そして、本実施の形態においては、1人のユーザが複数のIDを用いることを許容している。この結果、1人が複数の役職を有する場合に、各役職毎に異なる署名を1人のユーザが行うことが可能となる。

【0081】本実施の形態において特徴的なことは、1人のユーザが複数のIDを用いることが、システム上許容されていることである。

【0082】このような個人情報管理配列20aを用いているため、本実施の形態によれば、1人のユーザが複数の署名を使い分けることができ、利便性に富む署名処理を行うことができるのである。

【0083】さらに、本実施の形態においては、1つの秘密鍵を複数のユーザが共有することを許容している。すなわち、異なるIDを有する異なる人に対して、同一の鍵ハッシュ値を割り当てることにより、一つの秘密鍵を複数人が共同で使用することが可能となる。

【0084】例えば、上述した法人鍵等は複数人の取締役が使用する必要がある。そのような場合に、本実施の形態によれば、複数人の取締役が一つの法人鍵を共用することができるため、利便性の高いデジタル署名システムを実現することができる。

【0085】もちろん、このコンピュータを複数人で共有し、複数人が1台のコンピュータを使用する場合においても、各ユーザが個別の秘密鍵を有する場合だけでなく、1つの共通の鍵を複数人全員で共有して使用することも可能である。

【0086】図2(2)には、暗号鍵管理配列20bが示されている。この図に示されているように、暗号鍵管



理配列20bは、「鍵ハッシュ値」と、署名に用いる「秘密鍵」と、「クラス」が示されている。ここで、「鍵ハッシュ値」とは図2(1)で説明した鍵ハッシュ値であり、「クラス」とは秘密鍵の重要度を表すものであり、鍵を管理する際に用いられるデータである。このクラスは本発明にとっては必ずしも必須事項ではない。【0087】上述した個人情報管理配列20aを用いて、ユーザが使用する「ID」に従って、「鍵ハッシュ値」が求められる。この「鍵ハッシュ値」は、暗号鍵管理配列20bの内容を検索する際にキーとして用いられる。暗号鍵管理配列20bから、該当する「鍵ハッシュ値」が見いだされた場合には、対応する「秘密鍵」を暗号鍵管理配列20bから得ることができる。

【0088】このように、「鍵ハッシュ値」は、個人情報管理配列20aと、暗号鍵管理配列20bとを結びつけるキーとしての役割を果たす。そのため、本実施の形態においては、「鍵ハッシュ値」を用いたが、秘密鍵と対応していれば、単なる連続番号をハッシュ値の代わりに用いるのも好ましい。

【0089】また、本実施の形態においては、IDに関して正規化された配列と、秘密鍵に関して正規化された配列と、の2種類の配列を使用して、個人の管理と鍵の管理をそれぞれ別個独立に行っている。すなわち、本実施の形態に係るデジタル署名生成方法を実現するプログラムを利用する者が増えた場合には、個人情報管理配列20aを調整し、秘密鍵の種類が減った場合等には、暗号鍵管理配列20bのみを調整すればよく、効率の良い管理が行える。

【0090】しかし、上述したように、配列管理モジュール16の機能としては、IDから、そのIDに対応する登録動的署名データ及び秘密鍵が求められれば、十分である。従って、個人情報管理配列20aと、暗号鍵管理配列20bを統合して1つの配列を作り、その1つの配列で配列管理モジュール16に関する処理を行うことも可能である。

【0091】個人情報管理配列20aと暗号鍵管理配列20bとを統合すると、「鍵ハッシュ値」が省略されて、ユーザの「ID」、「登録動的署名データ」、「秘密鍵」、「クラス」の各項目を有する配列が1つ作成されることになる。

【0092】以上述べたように、本実施の形態において特徴的なことは、デジタル署名に用いられる秘密鍵を集中的に管理するプログラムを設けており、特に、このプログラム中に配列の形で秘密鍵を保存したので、プログラムの作成者以外の者がこのプログラム中の秘密鍵を削除したり、新たに付加したり、改竄を加えることは著しく困難である。

【0093】さらに、本実施の形態においては、本人であるかの特定のために生体署名データを使用した。そのため、本人であるとの特定をより正確なものとするこ

ができるため、第三者によるいわゆる「なりすまし」等を防止することができる。

【0094】そのため、本実施の形態に係るプログラムが第三者の手に渡っても、その第三者が悪意で秘密鍵を使用することはできず、また、プログラムの改竄による秘密鍵の悪用をすることも著しく困難となり、安全確実なデジタル署名を利用することができる。また、本実施の形態においては、複数人が1個の秘密鍵を共用すること、すなわち、1個の秘密鍵を複数人が共有することを許容しているため、法人鍵等の利用を円滑に行うことができる。更に、1人の人間が複数の秘密鍵を所有することをも許容しているため、役職毎に異なるデジタル署名をすることができる。

【0095】以上述べたように、本実施の形態は、以下のような特徴を有する。

【0096】(1) 生体署名データを使用するため、各人は一般のパスワードより短い自己のIDのみを認識していれば秘密鍵の使用ができる。

【0097】(2) 各ユーザがタブレット上で手で書く署名を行うことにより各ユーザが本人であるかの特定を行っているため、紙を利用して行われていた従来の署名行為から円滑に移行することができる。

【0098】(3) 必要に応じて認証に用いた「手で書いた署名データ」のイメージデータを利用することができる。従って、既存の手で行っていた署名行為との整合性や類似性を保存する事ができる。

【0099】

【発明の効果】以上述べたように本発明によれば、ユーザの特定を生体署名データで行ったため、本人の確認をより確実に行うことができる。

【0100】また、本発明によれば、複数のユーザが1つの秘密鍵を共有できるため、いわゆる法人鍵の管理がし易くなり、また、代理署名等が容易になるという効果を奏する。

【0101】また、本発明によれば、1人のユーザが複数の秘密鍵を所有できるため、1人のユーザが役職に応じて複数のデジタル署名を使い分けられることができるという効果を奏する。

【0102】また、本発明によれば、手で書く署名を生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【0103】また、本発明によれば、網膜パターンを生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【0104】また、本発明によれば、指紋を生体署名データとして用いたので本人か否かの検査を確実に行うことができる。

【0105】また、本発明によれば、手で書いた署名を表すイメージデータに対しても署名を施して出力するので、実際の手で書いた署名をイメージでとらえることが

できる。

【0106】また、本発明は、プログラムを格納したコンピュータ読みとり可能な記憶媒体であるため、秘密鍵の情報等をプログラム中に埋め込んで構成している。

【0107】したがって、本発明によれば、上で述べた各効果を奏すると共に、第三者にコピーされても未然に悪用を防止するという効果をも奏するのである。

【図面の簡単な説明】

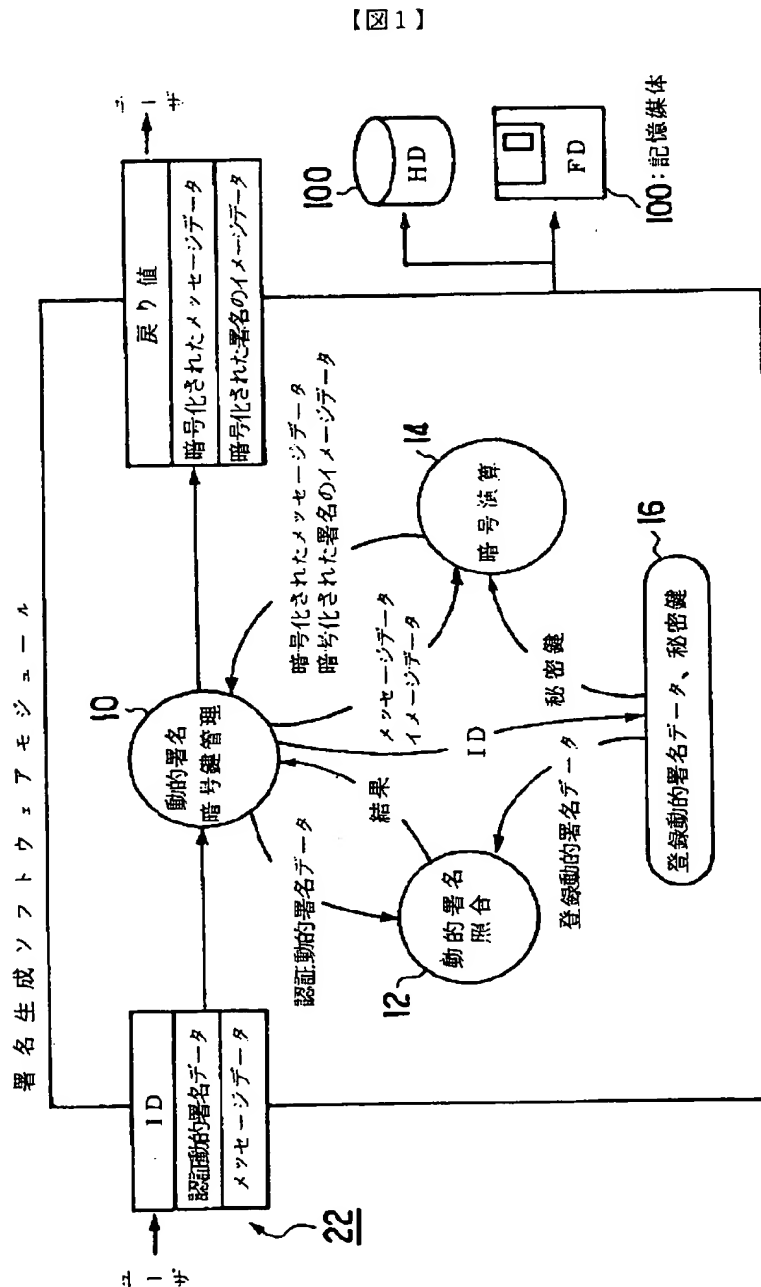
【図1】 本実施の形態に係るデジタル署名生成方法

の構成を表す説明図である。

【図2】 図1の配列管理モジュールの配列を表す説明図である。

【符号の説明】

10 動的署名暗号鍵管理モジュール、12 動的署名照合モジュール、14 暗号演算モジュール、16 配列管理モジュール、20a 個人情報管理配列、20b 暗号鍵管理配列、22 入力、100 記憶媒体。



【図2】

20a →

個人情報管理配列			
ID	登録時刻署名データ	鍵ハッシュ値	

&lt; 1 &gt;

20b ↙

暗号鍵管理配列			
鍵ハッシュ値	秘密鍵	クラス	

&lt; 2 &gt;